



DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 13, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

DOCKET FILE COPY ORIGINAL

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring ALL traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

No. of Copies rec'd _____
List ABCDE

Aug

Mr. William F. Canton

January 13, 1994

Page 2

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



Joyce Deeter

Telecommunications Manager

RECEIVED

JAN 19 1994

FCC MAIL ROOM

DOCKET FILE COPY ORIGINAL



CITY OF TEMPE

COMMUNICATIONS DIVISION
132 E. 6th Street; Suite B109
Tempe, AZ. 85280

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for the City of Tempe's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's, LEC's and CPE vendors to secure my systems, I have been a victim of toll fraud. Moreover, I can still experience toll fraud. It is impossible to secure my system 100 % from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100 % of our destiny. Since our destiny is not only controlled by our PBX precautions, but also by the information, services and equipment provided by IXC's, LEC's and CPE's, the law should reflect that. It is ludicrous to think that the IXC's, LEC's and CPE's who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPE's should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPE's ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPE's should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you purchase later.

No. of Copies rec'd Orig.
List ABCDE

While the programs offered by IXC's, such as AT&T NetProtect, MCI Detect and Sprint Guard have broken some new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for small users and the information is superficial. Monitoring by the IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

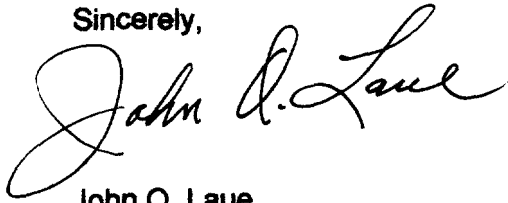
However, shared liability only addresses the symptom of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communications systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud. While it is the hacker who breaks in to the systems and sells the information, it is the call operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. Legislation must be developed that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this monumental problem.

Sincerely,

A handwritten signature in cursive script, reading "John O. Laue". The signature is fluid and elegant, with the first name "John" being larger and more prominent than the last name "Laue".

John O. Laue
Communications Engineering Manager
City of Tempe

cc: Patrick Flynn, Management Services Director



DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

SHERMAN TURNPIKE, DANBURY, CONNECTICUT 06816 • (203)797-3500 • CABLE: GROLIER DURY • TELEX: 969641

DOCKET FILE COPY ORIGINAL

January 13, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M. Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXC's LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default password which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software and in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXC's, such as MCI Detect, AT& T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd Orig.
List ABCDE

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



Karen J. Linstrum
Director, Telecommunications Services

KJL/jh



JAMES RIVER CORPORATION
WESTERN TRANSPORTATION
3710 NW Front Ave. Portland, OR 97210
P.O. Box 3869 Portland, OR 97208 (503) 294-8200

DO NOT FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

January 13, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd *Aug.*
List ABCDE

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



Wendy L. Weddle
Telecommunications Manager

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994



Champion

Champion International Corporation

FCC MAIL ROOM

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC'S and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken

No. of Copies rec'd
List ABCDE

Chiz

new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track

and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott Meyer", with a stylized flourish extending from the end.

Scott Meyer
Business Communications Engineer
Champion International Corporation

\mp

Baxter

January 13, 1994

DOCKET FILE COPY ORIGINAL
RECEIVED
JAN 19 1994
FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington D.C., 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning **Toll Fraud**. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXCs and CPE vendors to secure my systems, I still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided by the IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have no legal obligations to warn customers and therefore, no incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable

No. of Copies rec'd
List ABCDE

Orig.

Baxter

to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers (which was the case with my company's most recent toll fraud incident), the LEC's should be required to offer constant monitoring services similar to the IXC's.

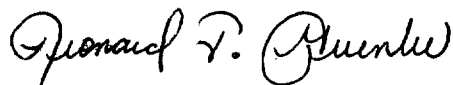
I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. If all parties have met the responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause. The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our systems. I do not believe it when the hackers state that they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks into the systems and sells the information, it is the call sell operations that profit from it.

Until we come up with an adequate method of law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute (to the fullest extent of the law) the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am sure that if we work together we can make a impact on this terrible problem.

Sincerely,



Leonard T. Greenlee
Manager, Administrative Services & Telecommunication
Baxter Biotech - Hyland Division

DOCKET FILE COPY ORIGINAL

January 11, 1994

RECEIVED
JAN 19 1994
FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Orig.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Jelly Smith
QVC Network, Inc.



City of Amarillo

RECEIVED

JAN 19 1994

FCC MAIL ROOM

COMMUNICATIONS

January 13, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

No. of Copies rec'd
List ABCDE

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXC's should be a part of the basic interchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



Walt Kelley
Communications Manager

RECEIVED

JAN 11 9 1994

FCC MAIL ROOM

DOCKET FILE COPY ORIGINAL

January 10, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because, even though I have taken every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment, and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment, with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by the IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard, have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd
List ABCDE

Orig.

As hackers begin new methods of breaking into systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the MPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll-fraud risks associated with features of the CPE, and the IXCs and LECS to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll-fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together, we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in cursive script, reading "Barbara Palant". The signature is written in dark ink and is positioned above the printed name and title.

Barbara Palant
Communications Consultant

BP:JS



Southwest Missouri State
U N I V E R S I T Y

Business Services
(417) 836-5100
Fax (417) 836-6583

January 12, 1994

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket #93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable. CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which as well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

Orig

Page 2

Mr. William F. Canton

January 12, 1994

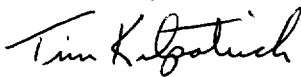
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the following:

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Tim Kilpatrick, Director
Business Services

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Chris

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Thomas Zover.
Telecom Supervisor / Charming S. HOPKES.

January 11, 1994

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 19 1994

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Orig.